

# **EXHIBIT D**

**Motion to Seal in the matter of Corbett v. TSA,  
No. 15-15717-D (11th Cir. 2016)**

IN THE UNITED STATES COURT OF APPEALS  
FOR THE ELEVENTH CIRCUIT

JONATHAN CORBETT,

Petitioner,

v.

TRANSPORTATION SECURITY  
ADMINISTRATION,

Respondent.

No. 15-15717-D

**MOTION FOR LEAVE TO FILE PORTIONS OF THE  
ADMINISTRATIVE RECORD UNDER SEAL AND PORTIONS  
*EX PARTE* AND UNDER SEAL**

## **CERTIFICATE OF INTERESTED PERSONS**

Pursuant to Eleventh Circuit Rule 26.1-1, the undersigned counsel certifies that, to the best of his knowledge, the following constitutes a complete list of the trial judge(s), all attorneys, persons, associations of persons, firms, partnerships, or corporations that have an interest in the outcome of the particular case or appeal:

Corbett, Jonathan

Mizer, Benjamin C.

Swingle, Sharon

Shih, Michael

/s/ Michael Shih

---

**MICHAEL SHIH**

*Counsel for the United States*

The government respectfully requests leave to file under seal the portions of the administrative record containing copyrighted and proprietary material. The government also requests leave to file *ex parte* and under seal the portions of the record containing material designated as For Official Use Only (“FOUO”) and that constitutes Sensitive Security Information (“SSI”). The government will file *ex parte* and *in camera* the portions of the administrative record containing classified information, and will file on the public docket the portions containing publicly accessible material. In support of this motion, the government states as follows:

1. This action arises from a petition for review filed by *pro se* petitioner Jonathan Corbett that names the Transportation Security Administration (“TSA”) as respondent. The petition seeks review of TSA’s decision to require certain airline passengers, as warranted by security considerations, to pass through scanners equipped with advanced imaging technology (“AIT”) at airport security checkpoints, without giving those passengers a right to decline AIT scanning in favor of an alternate method of screening. Per the Court’s Order of March 3, 2016, the certified index of record is due on May 2, 2016.

2. Petitioner previously brought in this Court an unsuccessful petition for review challenging TSA’s use of AIT scanners as a primary screening method at airport security checkpoints. *See Corbett v. TSA*, 767 F.3d 1171 (11th Cir. 2014). TSA filed an administrative record in the course of that lawsuit. That record

contained five categories of information: (1) publicly releasable documents (Volumes 1A-1C), (2) copyrighted and proprietary material (Volume 2); (3) documents designed as FOUO (Volume 3); (4) documents constituting SSI (Volumes 4A-4D); and (5) classified information (Volume 5). The government filed the portions of the record containing publicly accessible material on the public docket, and it filed the classified portions of the record *ex parte* and *in camera*.

In the prior action, TSA requested leave from this Court to file the copyrighted and FOUO portions of the record under seal, and the SSI portions of the record *ex parte* and under seal. As to the copyrighted and FOUO documents, the government offered to provide petitioner with copies of them on the condition that he sign a nondisclosure agreement. That agreement prohibited dissemination or use of the documents outside of the litigation, and obliged petitioner to safeguard the documents in accordance with Department of Homeland Security regulations. *See Corbett*, No. 12-15893, Mot. for Leave To File Portions of the Admin. Record Under Seal and Portions *Ex Parte* and Under Seal at 2-4 (11th Cir. Mar. 25, 2013). Petitioner opposed the government's request.

This Court temporarily granted the government's motion pending full briefing of petitioner's objections: (1) whether the copyrighted and proprietary material should remain under seal; (2) whether petitioner should be granted access

to SSI documents; and (3) whether the government should be required to file summaries or redacted versions of the classified portions of the record. *See Corbett*, No. 12-15893, Order at 1-3 (11th Cir. June 5, 2013). The Court required petitioner to sign a nondisclosure agreement as a condition of accessing the FOUO material. *Id.* at 2. Although the Court did not require petitioner to sign a nondisclosure agreement as a condition of receiving the copyrighted and proprietary material, it ordered petitioner to refrain from disclosing “any of the information contained in th[ose] documents” to the extent petitioner received them pursuant to the government’s filing of the administrative record. *Id.* But

Before oral argument, certain FOUO documents were inadvertently disclosed on the public docket by the Clerk of the Court. Petitioner “posted this privileged information on his blog” and “shar[ed] that information in an interview,” “likely breach[ing] his nondisclosure agreement” in the process. *Corbett*, 767 F.3d at 1184. In response, the Court ordered petitioner to “remove from his blog site any FOUO information or information derived from FOUO documents,” and directed petitioner “not to publish or publicly disclose any of the information in the FOUO documents” provided to him. *See Corbett*, No. 12-15893, Order at 2 (11th Cir. Jan. 17, 2014).

The Court ultimately ruled for the government on all three issues. *Corbett*, 767 F.3d at 1183. As to the copyrighted material, the Court noted that Eleventh

Circuit Rule 25-5 permits parties to file “proprietary or trade secret information” under seal, and that “every court of appeals in which [TSA] has submitted propriety information about the scanner technology has ordered it sealed.” *Id.* As to the SSI material, the Court held that petitioner “has no statutory or regulatory right to access” such material in a challenge to a TSA order filed directly in a court of appeals under 49 U.S.C. § 46110. *Id.* And as to the classified material, the Court held that petitioner had “fail[ed] to identify” any statute requiring the government to disclose summaries or redacted versions of classified documents to a civil litigant. *Id.* at 1183-84. In any event, petitioner “did not need the classified information to argue his case.” *Id.* at 1184.

3. The administrative record for this lawsuit is substantially similar to the record filed in petitioner’s previous lawsuit. This record—like that record—contains five categories of information: (1) publicly releasable documents (Volumes 1A-1C), (2) copyrighted material (Volume 2); (3) documents designated as FOUO (Volume 3); (4) documents constituting SSI (Volumes 4A-4D); and (5) classified information (Volume 5). The record differs only in that it contains additional documents of more recent vintage than 2013, when the previous record was filed.

a. *Publicly Releasable Documents.* Volumes 1A through 1C of the record are comprised of publicly releasable documents. The government is filing these volumes on the public docket concurrently with this motion.

b. *Copyrighted and Proprietary Documents.* Volume 2 consists of copyrighted documents that were provided to TSA through a single-user license. The volume also includes one proprietary document, an operations manual for an AIT scanner, which its owner has marked with the warning that customers “shall not disclose or transfer any of these materials or information to any third party” and that “[n]o part of this book may be reproduced in any form without written permission” from the company. *See Corbett*, 787 F.3d at 1183. The contents of Volume 2 have not changed from the volume’s previous iteration.

This Court previously permitted the government to file these same documents under seal. *Corbett*, 787 F.3d at 1183. There is no reason to deviate from that holding here. Sealing is appropriate under Eleventh Circuit Rule 25-5 to ensure compliance with the copyright laws and to protect the interests of the entity who owns the proprietary document. And every other circuit court in which this type of material has been filed has ordered it sealed. *See Redfern v. Napolitano*, No. 11-1805, Order (1st Cir. Aug. 14, 2012); *Elec. Privacy Information Ctr. v. U.S. DHS*, No. 10-1157, Order (D.C. Cir. Feb. 22, 2011).



The government stands ready to provide this volume to petitioner on the same terms that this Court allowed petitioner to access the volume the last time around. As noted above, this Court ordered petitioner to refrain from disclosing “any of the information contained in” the volume, but did not “limit his use of the documents” if petitioner obtained them “by any means other than this litigation.” *See Corbett*, No. 12-15893, Order at 1-2 (11th Cir. June 5, 2013). The government is satisfied that these conditions adequately balance the interests at stake.

c. *FOUO Documents*. Volume 3 contains two “Civil Aviation Threat Assessments”<sup>1</sup> that TSA has designated as FOUO. Its contents are unchanged from the previous iteration of the volume. These documents should be filed *ex parte* and under seal.

Per the Department of Homeland Security’s Management Directive 11042.1, *Safeguarding Sensitive But Unclassified (For Official Use Only) Information* (Exh. 1), documents designated as FOUO may be distributed only to individuals with a need to know the information. *See id.* at 8-9 ¶ 6(H). As explained in the attached declaration of Thomas Hoopes, Senior Intelligence Officer and Director of Intelligence Analysis for TSA’s Office of Intelligence and Analysis, “Civil

---

<sup>1</sup> The 2011 Civil Aviation Threat Assessment has been redacted to omit sensitive and privileged information not relevant to this case. TSA does not rely on that information in defending the challenged order.

Aviation Threat Assessments” are documents that “evaluate the risks presented by various entities and the vulnerabilities that terrorists and others might seek to exploit in order to harm the civil air transportation network.” Hoopes Decl. ¶ 4 (Exh. 2).<sup>2</sup> TSA has determined that these documents should be designated as FOUO and should not be publicly disclosed. Public disclosure “presents the real possibility that those intending to disrupt the nation’s civil aviation transportation system will be able to evaluate not only TSA’s perceived weaknesses, but also the extent to which TSA appears to be aware of their organizations and activities.” *Id.* ¶ 10. Disclosure could thus “create systemic vulnerabilities,” and could also “degrad[e] the information-sharing relationships TSA has developed with certain stakeholders.” *Id.* ¶ 11.

FOUO documents such as these threat assessments are properly filed under seal under Eleventh Circuit Rule 25-5, which sets forth many categories of sensitive information that can be redacted from the public record—including “national security information.” The sensitivity of these documents requires that they be filed under seal pursuant to a protective order.

---

<sup>2</sup> The government originally filed this declaration in *Redfern v. Napolitano*, No. 11-1805 (1st Cir.), a similar case challenging screening procedures at airport checkpoints. The government filed the declaration with this Court in a previous action brought by this petitioner. See *Corbett*, No. 12-15893 (11th Cir.).

Volume 3 should also be filed *ex parte*. Petitioner does not have a need to know the contents of the volume because he does not need them “to perform or assist in a lawful and authorized governmental function” or to “perform[] \* \* \* official duties.” Exh. 1, at 1-2. Although the government previously gave petitioner the privilege of access to these documents, that access was contingent upon petitioner’s execution of a nondisclosure agreement barring him from disseminating or using the documents outside that litigation, and obliging him to safeguard the material per Management Directive 11042.1. When the Clerk of this Court inadvertently placed FOUO material on the public docket, however, petitioner “post[ed] this privileged information on his blog and \* \* \* shar[ed] that information in an interview.” *Corbett*, 787 F.3d at 1184. By disseminating that information on the internet, petitioner “likely breached his nondisclosure agreement.” *Id.* In light of petitioner’s actions, the government seeks leave to file Volume 3 *ex parte*.

d. *SSI Documents*. Volumes 4A through 4D contain documents designated as SSI. These volumes contain the same SSI documents as Volumes 4A through 4D of the record filed in petitioner’s earlier lawsuit, as well as fifteen additional SSI documents. This Court previously granted the government’s motion to file SSI documents *ex parte* and under seal “because [petitioner] has no statutory or

regulatory right to access” them. *Corbett*, 787 F.3d at 1184. That conclusion applies with full force here.

Congress has directed TSA to “prescribe regulations prohibiting the disclosure of information obtained or developed in carrying out security \* \* \* if [TSA] decides that disclosing the information would \* \* \* be detrimental to the security of transportation.” 49 U.S.C. § 114(r)(1)(C). In response to that directive, TSA has defined a set of information as “Sensitive Security Information” (“SSI”) that may not be disclosed except in certain limited circumstances. 49 C.F.R. § 1520.5 (describing information that constitutes SSI); *id.* § 1520.9(a)(2) (explaining that SSI may generally be disclosed only to “covered persons who have a need to know”); *id.* § 1520.7 (defining “[c]overed persons”); *id.* § 1520.11 (defining “need to know”).

TSA has reviewed the record in this case and has determined that the documents appearing in Volumes 4A through 4D constitute SSI. Those documents will be filed with the Court pursuant to 49 C.F.R. §§ 1520.7(j), 1520.9(a)(2), and 1520.11(b)(1), which provide for the disclosure of SSI to government employees who have a need to know the information because access to the information is necessary for the performance of their official duties.<sup>3</sup> Eleventh Circuit Rule 25-5

---

<sup>3</sup> The Court’s handling of SSI is governed by 49 C.F.R. Part 1520. For the Court’s guidance and convenience, we are attaching as Exhibit 3 a one-page

recognizes that SSI is properly filed under seal. In addition, because petitioner is not a “covered person” with a “need to know” SSI within the meaning of 49 C.F.R. §§ 1520.7, 1520.9(a)(2), and 1520.11, Volumes 4A-4D should be filed *ex parte*—just as similar SSI portions of the administrative record were previously filed in this Court as to this petitioner, *see Corbett*, 787 F.3d at 1183, and just as they were filed in other courts, *see, e.g., Redfern v. Napolitano*, No. 11-1805, Order (1st Cir. Aug. 14, 2012) (granting leave to file SSI documents *ex parte* and under seal).

TSA is in the process of creating a redacted, publicly releasable version of the SSI documents in the administrative record. That process is not yet finished. Once redactions are complete, and within 45 days of the Court’s ruling on this motion, the government will file a public version of the SSI portions of the record with the Court.

5. *Classified Information.* Volume 5 of the administrative record contains the same classified documents filed in petitioner’s previous lawsuit, as well as several additional classified documents. The handling of classified information is governed by federal law. *See, e.g.,* Exec. Order No. 13,526; 75 Fed. Reg. 707 (Dec. 29, 2009). Federal law prohibits disclosure of classified information except

---

document, TSA’s “Best Practices Guide,” summarizing the proper handling of SSI material by the Court.

to individuals who have been cleared for access to the information by the head of a federal agency or his designee; who have signed a nondisclosure agreement; and who have a need-to-know the information. *See id.* § 4.1(a); 75 Fed. Reg. at 720. Accordingly, the classified portions of the record may not be disclosed to the public or to petitioner, who has not been cleared for access to classified information. The classified portion of the record should be filed by the Court *in camera* and *ex parte*. At the Court's direction, Volume 5 will be filed through the Court Security Officer.

## CONCLUSION

For these reasons, the Court should grant respondent leave to file the copyrighted and proprietary portions of the administrative record under seal. The Court should also grant respondent leave to file the FOUO and SSI portions of the administrative record *ex parte* and under seal. In addition, and at the Court's direction, respondent will file the classified information with the Court *ex parte* and *in camera*.

Respectfully submitted,

SHARON SWINGLE

/s/ Michael Shih  
MICHAEL SHIH  
(202) 353-6880  
Attorneys, Appellate Staff  
Civil Division  
U.S. Department of Justice  
950 Pennsylvania Ave., N.W.  
Room 7268  
Washington, D.C. 20530  
*Counsel for the United States*

MAY 2016

### **CERTIFICATE OF SERVICE**

I hereby certify that on May 2, 2016, I filed the foregoing motion with the Clerk of the Court by electronic delivery. I served the following party with the foregoing motion by electronic delivery:

Jonathan Corbett  
382 N.E. 191st St., #86952  
Miami, FL 33179  
jon@professional-troublemaker.com

/s/ Michael Shih

MICHAEL SHIH

*Counsel for the United States*



**EXHIBIT 1**

Department of Homeland Security  
Management Directive System  
MD Number: 11042.1

# **SAFEGUARDING SENSITIVE BUT UNCLASSIFIED (FOR OFFICIAL USE ONLY) INFORMATION**

1.6.2005

---

## **1. Purpose**

This directive establishes Department of Homeland Security (DHS) policy regarding the identification and safeguarding of sensitive but unclassified information originated within DHS. It also applies to other sensitive but unclassified information received by DHS from other government and non-governmental activities.

## **2. Scope**

This directive is applicable to all DHS Headquarters, components, organizational elements, detailees, contractors, consultants, and others to whom access to information covered by this directive is granted.

## **3. Authorities**

Homeland Security Act of 2002.

## **4. Definitions**

**Access:** The ability or opportunity to gain knowledge of information.

**For Official Use Only (FOUO):** The term used within DHS to identify unclassified information of a sensitive nature, not otherwise categorized by statute or regulation, the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national interest. Information impacting the National Security of the United States and classified Confidential, Secret, or Top Secret under Executive Order 12958, "Classified National Security Information," as amended, or its predecessor or successor orders, is not to be considered FOUO. FOUO is not to be considered classified information.

**Need-to-know:** The determination made by an authorized holder of information that a prospective recipient requires access to specific information in order to

perform or assist in a lawful and authorized governmental function, i.e., access is required for the performance of official duties.

**Organizational Element:** As used in this directive, organizational element is as defined in DHS MD Number 0010.1, Management Directive System and DHS Announcements.

**Protected Critical Infrastructure Information (PCII):** Critical infrastructure information (CII) is defined in 6 U.S.C. 131(3) (Section 212(3) of the Homeland Security Act). Critical infrastructure information means information not customarily in the public domain and related to the security of critical infrastructure or protected systems. Protected Critical Infrastructure Information is a subset of CII that is voluntarily submitted to the Federal Government and for which protection is requested under the PCII program by the requestor.

**Sensitive Security Information (SSI):** Sensitive security information (SSI) is defined in 49 C.F.R. Part 1520. SSI is a specific category of information that requires protection against disclosure. 49 U.S.C. 40119 limits the disclosure of information obtained or developed in carrying out certain security or research and development activities to the extent that it has been determined that disclosure of the information would be an unwarranted invasion of personal privacy; reveal a trade secret or privileged or confidential commercial or financial information; or be detrimental to the safety of passengers in transportation.

## 5. Responsibilities

### A. The DHS Office of Security will:

1. Be responsible for practical application of all aspects of the program to protect FOUO.
2. Promulgate Department-wide policy guidance.
3. Develop and implement an education and awareness program for the safeguarding of FOUO and other sensitive but unclassified information.

### B. Heads of DHS Organizational Elements will:

1. Ensure compliance with the standards for safeguarding FOUO and other sensitive but unclassified information as cited in this directive.
2. Designate an official to serve as a Security Officer or Security Liaison.

### C. The organizational element's Security Officer/Security Liaison will:

Be responsible for implementation and oversight of the FOUO information protection program and will serve as liaison between the DHS Office of Security and other organizational security officers.

D. DHS employees, detailees, contractors, consultants and others to whom access is granted will:

1. Be aware of and comply with the safeguarding requirements for FOUO information as outlined in this directive.
2. Participate in formal classroom or computer based training sessions presented to communicate the requirements for safeguarding FOUO and other sensitive but unclassified information.
3. Be aware that divulging information without proper authority could result in administrative or disciplinary action.

E. Contractors and Consultants shall:

Execute a DHS Form 11000-6, Sensitive But Unclassified Information Non-Disclosure Agreement (NDA), as a condition of access to such information. Other individuals not assigned to or contractually obligated to DHS, but to whom access to information will be granted, may be requested to execute an NDA as determined by the applicable program manager. Execution of the NDA shall be effective upon publication of this directive and not applied retroactively.

F. Supervisors and managers will:

1. Ensure that an adequate level of education and awareness is established and maintained that serves to emphasize safeguarding and prevent unauthorized disclosure of FOUO information.
2. Take appropriate corrective actions, to include administrative or disciplinary action as appropriate, when violations occur.

## **6. Policy and Procedures**

A. General

1. The Computer Security Act of 1987, Public Law 100-235, defines "sensitive information" as "any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, United States Code (the Privacy Act) but which has not been specifically authorized under criteria established by an executive

order or an act of Congress to be kept secret in the interest of national defense or foreign policy.” However, with the exception of certain types of information protected by statute, specific, standard criteria and terminology defining the types of information warranting designation as “sensitive information” does not exist within the Federal government. Such designations are left to the discretion of each individual agency.

2. Within the “sensitive but unclassified” arena, in addition to the various categories of information specifically described and protected by statute or regulation, e.g., Tax Return Information, Privacy Act Information, Sensitive Security Information (SSI), Critical Infrastructure Information (CII), Grand Jury Information, etc. There are numerous additional caveats used by various agencies to identify unclassified information as sensitive, e.g., For Official Use Only; Law Enforcement Sensitive; Official Use Only; Limited Official Use; etc. Regardless of the caveat used to identify it, however, the reason for the designation does not change. Information is designated as sensitive to control and restrict access to certain information, the release of which could cause harm to a person’s privacy or welfare, adversely impact economic or industrial institutions, or compromise programs or operations essential to the safeguarding of our national interests.

3. Information shall not be designated as FOUO in order to conceal government negligence, ineptitude, illegalities, or other disreputable circumstances embarrassing to a government agency.

4. Information designated as FOUO is not automatically exempt from disclosure under the provisions of the Freedom of Information Act, 5 U.S.C. 552, (FOIA). Information requested by the public under a FOIA request must still be reviewed on a case-by-case basis.

#### B. For Official Use Only

Within DHS, the caveat “FOR OFFICIAL USE ONLY” will be used to identify sensitive but unclassified information within the DHS community that is not otherwise specifically described and governed by statute or regulation. The use of these and other approved caveats will be governed by the statutes and regulations issued for the applicable category of information.

#### C. Information Designated as FOUO

1. The following types of information will be treated as FOUO information. Where information cited below also meets the standards for designation pursuant to other existing statutes or regulations, the applicable statutory or regulatory guidance will take precedence. For example, should information meet the standards for designation as Sensitive Security Information (SSI), then SSI guidance for marking, handling, and safeguarding will take precedence.

- (a) Information of the type that may be exempt from disclosure per 5 U.S.C. 552, Freedom of Information Act, and its amendments. Designation of information as FOUO does not imply that the information is already exempt from disclosure under FOIA. Requests under FOIA, for information designated as FOUO, will be reviewed and processed in the same manner as any other FOIA request.
- (b) Information exempt from disclosure per 5 U.S.C. 552a, Privacy Act.
- (c) Information within the international and domestic banking and financial communities protected by statute, treaty, or other agreements.
- (d) Other international and domestic information protected by statute, treaty, regulation or other agreements.
- (e) Information that could be sold for profit.
- (f) Information that could result in physical risk to personnel.
- (g) DHS information technology (IT) internal systems data revealing infrastructure used for servers, desktops, and networks; applications name, version and release; switching, router, and gateway information; interconnections and access methods; mission or business use/need. Examples of information are systems inventories and enterprise architecture models. Information pertaining to national security systems and eligible for classification under Executive Order 12958, as amended, will be classified as appropriate.
- (h) Systems security data revealing the security posture of the system. For example, threat assessments, system security plans, contingency plans, risk management plans, Business Impact Analysis studies, and Certification and Accreditation documentation.
- (i) Reviews or reports illustrating or disclosing facility infrastructure or security vulnerabilities, whether to persons, systems, or facilities, not otherwise eligible for classification under Executive Order 12958, as amended.
- (j) Information that could constitute an indicator of U.S. government intentions, capabilities, operations, or activities or otherwise threaten operations security.
- (k) Developing or current technology, the release of which could hinder the objectives of DHS, compromise a technological advantage or countermeasure, cause a denial of service, or provide an adversary with



sufficient information to clone, counterfeit, or circumvent a process or system.

2. Other government agencies and international organizations may use different terminology to identify sensitive information, such as "Limited Official Use (LOU)," and "Official Use Only (OUO)." In most instances the safeguarding requirements for this type of information are equivalent to FOUO. However, other agencies and international organizations may have additional requirements concerning the safeguarding of sensitive information. Follow the safeguarding guidance provided by the other agency or organization. Should there be no such guidance, the information will be safeguarded in accordance with the requirements for FOUO as provided in this manual. Should the additional guidance be less restrictive than in this directive, the information will be safeguarded in accordance with this directive.

#### D. Designation Authority

Any DHS employee, detailee, or contractor can designate information falling within one or more of the categories cited in section 6, paragraph C, as FOUO. Officials occupying supervisory or managerial positions are authorized to designate other information, not listed above and originating under their jurisdiction, as FOUO.

#### E. Duration of Designation

Information designated as FOUO will retain its designation until determined otherwise by the originator or a supervisory or management official having program management responsibility over the originator and/or the information.

#### F. Marking

1. Information designated as FOUO will be sufficiently marked so that persons having access to it are aware of its sensitivity and protection requirements. The lack of FOUO markings on materials does not relieve the holder from safeguarding responsibilities. Where the FOUO marking is not present on materials known by the holder to be FOUO, the holder of the material will protect it as FOUO. Other sensitive information protected by statute or regulation, e.g., PCII and SSI, etc., will be marked in accordance with the applicable guidance for that type of information. Information marked in accordance with the guidance provided for the type of information need not be additionally marked FOUO.

(a) Prominently mark the bottom of the front cover, first page, title page, back cover and each individual page containing FOUO information with the caveat "FOR OFFICIAL USE ONLY."

(b) Materials containing specific types of FOUO may be further marked with the applicable caveat, e.g., "LAW ENFORCEMENT SENSITIVE," in order to alert the reader of the type of information conveyed. Where the sensitivity of the information warrants additional access and dissemination restrictions, the originator may cite additional access and dissemination restrictions. For example:

***WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.***

(c) Materials being transmitted to recipients outside of DHS, for example, other federal agencies, state or local officials, etc. who may not be aware of what the FOUO caveat represents, shall include the following additional notice:

***WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.***

(d) Computer storage media, i.e., disks, tapes, removable drives, etc., containing FOUO information will be marked "FOR OFFICIAL USE ONLY."

(e) Portions of a classified document, i.e., subjects, titles, paragraphs, and subparagraphs that contain only FOUO information will be marked with the abbreviation (FOUO).

(f) Individual portion markings on a document that contains no other designation are not required.

(g) Designator or originator information and markings, downgrading instructions, and date/event markings are not required.

#### G. General Handling Procedures

Although FOUO is the DHS standard caveat for identifying sensitive unclassified information, some types of FOUO information may be more sensitive than others



and thus warrant additional safeguarding measures beyond the minimum requirements established in this manual. For example, certain types of information may be considered extremely sensitive based on the repercussions that could result should the information be released or compromised. Such repercussions could be the loss of life or compromise of an informant or operation. Additional control requirements may be added as necessary to afford appropriate protection to the information. DHS employees, contractors, and detailees must use sound judgment coupled with an evaluation of the risks, vulnerabilities, and the potential damage to personnel or property as the basis for determining the need for safeguards in excess of the minimum requirements and protect the information accordingly.

1. When removed from an authorized storage location (see section 6.I) and persons without a need-to-know are present, or where casual observation would reveal FOUO information to unauthorized persons, a "FOR OFFICIAL USE ONLY" cover sheet (Enclosure 1) will be used to prevent unauthorized or inadvertent disclosure.
2. When forwarding FOUO information, a FOUO cover sheet should be placed on top of the transmittal letter, memorandum or document.
3. When receiving FOUO equivalent information from another government agency, handle in accordance with the guidance provided by the other government agency. Where no guidance is provided, handle in accordance with the requirements of this directive.

#### H. Dissemination and Access

1. FOUO information will not be disseminated in any manner - orally, visually, or electronically - to unauthorized personnel.
2. Access to FOUO information is based on "need-to-know" as determined by the holder of the information. Where there is uncertainty as to a person's need-to-know, the holder of the information will request dissemination instructions from their next-level supervisor or the information's originator.
3. The holder of the information will comply with any access and dissemination restrictions.
4. A security clearance is not required for access to FOUO information.
5. When discussing or transferring FOUO information to another individual(s), ensure that the individual with whom the discussion is to be held or the information is to be transferred has a valid need-to-know, and that precautions are taken to prevent unauthorized individuals from overhearing the conversation, observing the materials, or otherwise obtaining the information.

6. FOUO information may be shared with other agencies, federal, state, tribal, or local government and law enforcement officials, provided a specific need-to-know has been established and the information is shared in furtherance of a coordinated and official governmental activity. Where FOUO information is requested by an official of another agency and there is no coordinated or other official governmental activity, a written request will be made from the requesting agency to the applicable DHS program office providing the name(s) of personnel for whom access is requested, the specific information to which access is requested, and basis for need-to-know. The DHS program office shall then determine if it is appropriate to release the information to the other agency official. (see section 6.F for marking requirements)
7. Other sensitive information protected by statute or regulation, i.e., Privacy Act, CII, SSI, Grand Jury, etc., will be controlled and disseminated in accordance with the applicable guidance for that type of information.
8. If the information requested or to be discussed belongs to another agency or organization, comply with that agency's policy concerning third party discussion and dissemination.
9. When discussing FOUO information over a telephone, the use of a STU III (Secure Telephone Unit), or Secure Telephone Equipment (STE), is encouraged, but not required.

#### I. Storage

1. When unattended, FOUO materials will, at a minimum, be stored in a locked file cabinet, locked desk drawer, a locked overhead storage compartment such as a systems furniture credenza, or similar locked compartment. Materials can also be stored in a room or area that has sufficient physical access control measures to afford adequate protection and prevent unauthorized access by members of the public, visitors, or other persons without a need-to-know, such as a locked room, or an area where access is controlled by a guard, cipher lock, or card reader.
2. FOUO information will not be stored in the same container used for the storage of classified information unless there is a correlation between the information. When FOUO materials are stored in the same container used for the storage of classified materials, they will be segregated from the classified materials to the extent possible, i.e. separate folders, separate drawers, etc.
3. IT systems that store FOUO information will be certified and accredited for operation in accordance with federal and DHS standards. Consult the DHS Information Technology Security Program Handbook for Sensitive Systems, Publication 4300A, for more detailed information.

4. Laptop computers and other media containing FOUO information will be stored and protected to prevent loss, theft, unauthorized access and unauthorized disclosure. Storage and control will be in accordance with DHS Information Technology Security Program Handbook for Sensitive Systems, Publication 4300A.

#### J. Transmission

1. Transmission of hard copy FOUO within the U.S. and its Territories:
  - (a) Material will be placed in a single opaque envelope or container and sufficiently sealed to prevent inadvertent opening and to show evidence of tampering. The envelope or container will bear the complete name and address of the sender and addressee, to include program office and the name of the intended recipient (if known).
  - (b) FOUO materials may be mailed by U.S. Postal Service First Class Mail or an accountable commercial delivery service such as Federal Express or United Parcel Service.
  - (c) FOUO materials may be entered into an inter-office mail system provided it is afforded sufficient protection to prevent unauthorized access, e.g., sealed envelope.
2. Transmission to Overseas Offices: When an overseas office is serviced by a military postal facility, i.e., APO/FPO, FOUO may be transmitted directly to the office. Where the overseas office is not serviced by a military postal facility, the materials will be sent through the Department of State, Diplomatic Courier.
3. Electronic Transmission.
  - (a) Transmittal via Fax. Unless otherwise restricted by the originator, FOUO information may be sent via nonsecure fax. However, the use of a secure fax machine is highly encouraged. Where a nonsecure fax is used, the sender will coordinate with the recipient to ensure that the materials faxed will not be left unattended or subjected to possible unauthorized disclosure on the receiving end. The holder of the material will comply with any access, dissemination, and transmittal restrictions cited on the material or verbally communicated by the originator.
  - (b) Transmittal via E-Mail
    - (i) FOUO information transmitted via email should be protected by encryption or transmitted within secure communications systems. When this is impractical or unavailable, FOUO may be transmitted over regular email channels. For added security, when

transmitting FOUO over a regular email channel, the information can be included as a password protected attachment with the password provided under separate cover. Recipients of FOUO information will comply with any email restrictions imposed by the originator.

(ii) Per DHS MD 4300, DHS Sensitive Systems Handbook, due to inherent vulnerabilities, FOUO information shall not be sent to personal email accounts.

(c) DHS Internet/Intranet

(i) FOUO information will not be posted on a DHS or any other internet (public) website.

(ii) FOUO information may be posted on the DHS intranet or other government controlled or sponsored protected encrypted data networks, such as the Homeland Security Information Network (HSIN). However, the official authorized to post the information should be aware that access to the information is open to all personnel who have been granted access to that particular intranet site. The official must determine the nature of the information is such that need-to-know applies to all personnel; the benefits of posting the information outweigh the risk of potential compromise; the information posted is prominently marked as FOR OFFICIAL USE ONLY; and information posted does not violate any provisions of the Privacy Act.

K. Destruction

1. FOUO material will be destroyed when no longer needed. Destruction may be accomplished by:

(a) "Hard Copy" materials will be destroyed by shredding, burning, pulping, pulverizing, such as to assure destruction beyond recognition and reconstruction. After destruction, materials may be disposed of with normal waste.

(b) Electronic storage media shall be sanitized appropriately by overwriting or degaussing. Contact local IT security personnel for additional guidance.

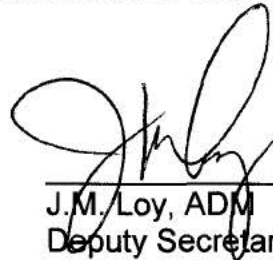
(c) Paper products containing FOUO information will not be disposed of in regular trash or recycling receptacles unless the materials have first been destroyed as specified above.

L. Incident Reporting

1. The loss, compromise, suspected compromise, or unauthorized disclosure of FOUO information will be reported. Incidents involving FOUO in DHS IT systems will be reported to the organizational element Computer Security Incident Response Center in accordance with IT incident reporting requirements.
2. Suspicious or inappropriate requests for information by any means, e.g., email or verbal, shall be report to the DHS Office of Security.
3. Employees or contractors who observe or become aware of the loss, compromise, suspected compromise, or unauthorized disclosure of FOUO information will report it immediately, but not later than the next duty day, to the originator and the local Security Official.
4. Additional notifications to appropriate DHS management personnel will be made without delay when the disclosure or compromise could result in physical harm to an individual(s) or the compromise of a planned or on-going operation.
5. At the request of the originator, an inquiry will be conducted by the local security official or other designee to determine the cause and affect of the incident and the appropriateness of administrative or disciplinary action against the offender.

Dated: \_\_\_\_\_

1/6/05



\_\_\_\_\_  
J.M. Loy, ADM  
Deputy Secretary of Homeland Security

# **Department of Homeland Security**

## **FOR OFFICIAL USE ONLY**

**THE ATTACHED MATERIALS CONTAIN DEPARTMENT OF HOMELAND SECURITY INFORMATION THAT IS "FOR OFFICIAL USE ONLY," OR OTHER TYPES OF SENSITIVE BUT UNCLASSIFIED INFORMATION REQUIRING PROTECTION AGAINST UNAUTHORIZED DISCLOSURE. THE ATTACHED MATERIALS WILL BE HANDLED AND SAFEGUARDED IN ACCORDANCE WITH DHS MANAGEMENT DIRECTIVES GOVERNING PROTECTION AND DISSEMINATION OF SUCH INFORMATION.**

**AT A MINIMUM, THE ATTACHED MATERIALS WILL BE DISSEMINATED ONLY ON A "NEED-TO-KNOW" BASIS AND WHEN UNATTENDED, WILL BE STORED IN A LOCKED CONTAINER OR AREA OFFERING SUFFICIENT PROTECTION AGAINST THEFT, COMPROMISE, INADVERTENT ACCESS AND UNAUTHORIZED DISCLOSURE.**

**EXHIBIT 2**



**IN THE UNITED STATES COURT OF APPEALS  
FOR THE FIRST CIRCUIT**

JEFFREY H. REDFERN; )  
ANANT N. PRADHAN, )  
Plaintiffs-Appellants, )  
)  
v. )  
)  
JANET NAPOLITANO, in her official ) No. 11-1805  
capacity as Secretary of Homeland )  
Security; JOHN PISTOLE, in his official )  
capacity as Administrator of the )  
Transportation Security Administration, )  
Defendants-Appellees. )  
)  
)

**DECLARATION OF THOMAS HOOPES IN SUPPORT  
OF DEFENDANTS-APPELLEES' MOTION TO FILE PORTIONS OF  
THE ADMINISTRATIVE RECORD UNDER SEAL**

THOMAS B. HOOPES hereby declares, pursuant to 28 U.S.C. § 1746, as follows:

1. I am the Senior Intelligence Officer and Director of Intelligence Analysis for the Transportation Security Administration's (TSA) Office of Intelligence and Analysis (OIA). I joined TSA in 2005 and have served in my present capacity since 2011. As Director of Intelligence Analysis, I am responsible for gathering, evaluating and disseminating within TSA intelligence regarding threats to national transportation systems, including the civil aviation system. The statements in this declaration are based upon my



personal knowledge and information obtained by me in the course of my official duties.

2. The mission of OIA is to efficiently and effectively receive, assess, and distribute actionable intelligence and vetting information related to transportation security in order to equip security professionals focused on this sector with timely and relevant information needed to prevent or mitigate threats to transportation.

3. Within OIA, I serve as the principal intelligence expert for the Assistant Administrator and Deputy Assistant Administrator regarding the development and oversight of Trend Analysis, Situational Analysis, and Production Management.

4. Among the products for which my Branch within OIA is responsible are Civil Aviation Threat Assessments (CATAs), which are issued regularly and evaluate the risks presented by various entities and the vulnerabilities that terrorists and others might seek to exploit in order to harm the civil air transportation network.

5. In order to ensure that OIA's CATAs are available to the wide array of security professionals, OIA has issued these documents in a non-classified format.

6. The level of analysis contained within OIA's CATAs is nevertheless very sensitive, as demonstrated by the fact that the June 1, 2010 CATA was determined to be Sensitive Security Information (SSI) as defined by 49 U.S.C. § 114(r) and 49 C.F.R. part 1520.

7. OIA has designated the CATA for 2008, issued on March 20, 2008, as For Official Use Only (FOUO). OIA has designated the CATA for 2011, issued on October 12, 2011, as Law Enforcement Sensitive (LES) and FOUO, but it is my understanding that the LES information in the CATA for 2011 has been redacted for purposes of inclusion in the administrative record in the above-captioned case.

8. For all information designated as FOUO, a determination has been made that "the unauthorized disclosure of [the information] could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national interest." Department of Homeland Security, *Safeguarding Sensitive But Unclassified (For Official Use Only) Information*, Management Directive 11042.1, at 1 ¶ 4. Pursuant to the governing management directive, FOUO information must be handled, stored, disseminated, and transmitted in specified ways that safeguard the information. *See id.* at 6-12 ¶ 6(F)-(L). As relevant here, FOUO information may be

distributed only to individuals with a need-to-know the information. *See id.* at 8-9 ¶ 6(H).

9. In determining that the CATAs for 2008 and 2011 should be designated as FOUO, OIA concluded that limited restrictions on the dissemination of these particular intelligence assessments struck the necessary balance between ensuring that these vital products were sufficiently available to transportation security professionals, and yet were not freely available to those who might exploit the analysis and assessment contained therein to undermine transportation security.

10. The unrestricted dissemination of CATAs presents the real possibility that those intending to disrupt the nation's civil aviation transportation system will be able to evaluate not only TSA's perceived weaknesses, but also the extent to which TSA appears to be aware of their organizations and activities.

11. Unrestricted dissemination of CATAs could, therefore, create systemic vulnerabilities, by affording the entities identified therein a clearer understanding of TSA's analysis of threat information and priorities, as well as by degrading the information-sharing relationships TSA has developed with certain stakeholders.

12. In creating and distributing CATAs, OIA expects that those within TSA and TSA's partners will ensure that these products are not freely available and

are handled in accordance with the Department of Homeland Security's Management Directive 11042.1 where applicable.

13. For these reasons, it is important that, notwithstanding their use in this litigation, the CATAs referenced in Paragraph 7 not be filed on the public docket. It is also important that plaintiffs be prohibited from disseminating CATAs or any information contained therein, and that plaintiffs treat the CATAs in accordance with the requirements outlined in the Department of Homeland Security's Management Directive 11042.1.


///

///

///

I declare under penalty of perjury that the foregoing is true and correct.

Executed July 6, 2012  
Arlington, Virginia

  
\_\_\_\_\_  
Thomas B. Hoopes  
Director of Intelligence Analysis  
Transportation Security Administration  
U.S. Department of Homeland Security

**EXHIBIT 3**





# Sensitive Security Information

## Best Practices Guide for Non-DHS Employees

The purpose of this hand-out is to provide *transportation security stakeholders and non-DHS government employees and contractors* with best practices for handling SSI. Best practices are not to be construed as legally binding requirements of, or official implementing guidance for, the SSI regulation.

### What is SSI?

Sensitive Security Information (SSI) is information that, if publicly released, would be *detrimental to transportation security*, as defined by Federal regulation 49 C.F.R. part 1520.

Although SSI is not classified information, there are specific procedures for recognizing, marking, protecting, safely sharing, and destroying SSI. As persons receiving SSI in order to carry out responsibilities related to transportation security, you are considered "covered persons" under the SSI regulation and have special obligations to protect this information from unauthorized disclosure.

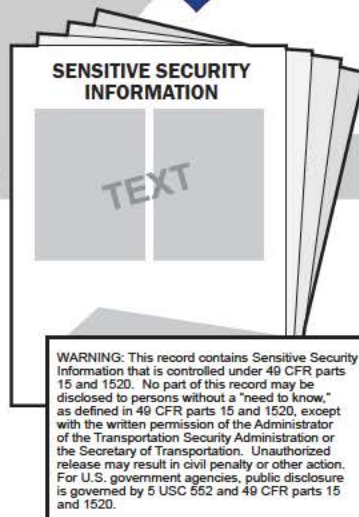
### SSI Requirements

The SSI regulation mandates specific and general requirements for handling and protecting SSI.

**You Must – Lock Up All SSI:** Store SSI in a secure container such as a locked file cabinet or drawer (as defined by Federal regulation 49 C.F.R. part 1520.9 (a)(1)).

**You Must – When No Longer Needed, Destroy SSI:** Destruction of SSI must be complete to preclude recognition or reconstruction of the information (as defined by Federal regulation 49 C.F.R. part 1520.19).

**You Must – Mark SSI:** The regulation requires that even when only a small portion of a paper document contains SSI, every page of the document must be marked with the SSI header and footer shown at left (as defined by Federal regulation 49 C.F.R. part 1520.13). Alteration of the footer is not authorized.



## Best Practices Guide

Reasonable steps must be taken to safeguard SSI. While the regulation does not define reasonable steps, the TSA SSI Branch offers these best practices as examples of reasonable steps:

- ★ Use an SSI cover sheet on all SSI materials.
- ★ Electronic presentations (e.g., PowerPoint) should be marked with the SSI header on all pages and the SSI footer on the first and last pages of the presentation.
- ★ Spreadsheets should be marked with the SSI header on every page and the SSI footer on every page or at the end of the document.
- ★ Video and audio should be marked with the SSI header and footer on the protective cover when able and the header and footer should be shown and/or read at the beginning and end of the program.
- ★ CDs/DVDs should be encrypted or password-protected and the header and footer should be affixed to the CD/DVD.
- ★ Portable drives including "flash" or "thumb" drives should not themselves be marked, but the drive itself should be encrypted or all SSI documents stored on it should be password protected.
- ★ When leaving your computer or desk you must lock up all SSI and you should lock or turn off your computer.
- ★ Taking SSI home is not recommended. If necessary, get permission from a supervisor and lock up all SSI at home.
- ★ Don't handle SSI on computers that have peer-to-peer software installed on them or on your home computer.
- ★ Transmit SSI via email only in a password protected attachment, not in the body of the email. Send the password without identifying information in a separate email or by phone.
- ★ Passwords for SSI documents should contain at least eight characters, have at least one uppercase and one lowercase letter, contain at least one number, one special character and not be a word in the dictionary.
- ★ Faxing of SSI should be done by first verifying the fax number and that the intended recipient will be available promptly to retrieve the SSI.
- ★ SSI should be mailed by U.S. First Class mail or other traceable delivery service using an opaque envelope or wrapping. The outside wrapping (i.e. box or envelope) should not be marked as SSI.
- ★ Interoffice mail should be sent using an unmarked, opaque, sealed envelope so that the SSI cannot be read through the envelope.
- ★ SSI stored in network folders should either require a password to open or the network should limit access to the folder to only those with a need to know.
- ★ Properly destroy SSI using a cross-cut shredder or by cutting manually into less than ½ inch squares.
- ★ Properly destroy electronic records using any method that will preclude recognition or reconstruction.